HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200209600-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Mendonca, et al.	Confirmation No.:	3688
Application No.:	10/627,017	Examiner:	Okoronkwo, C.
Filing Date:	07/25/2003	Group Art Unit:	2136

Title: METHOD OF MANAGING UTILIZATION OF NETWORK INTRUSION DETECTION SYSTEMS IN A DYNAMIC DATA CENTER

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 9/12/2007.

☒ The fee for filing this Appeal Brief is $510.00 (37 CFR 41.20).

☒ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $460	☐ 3rd Month $1050	☐ 4th Month $1640

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 510. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: 11/09/2007

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Ilene L. Fish
Signature:

Respectfully submitted,

Mendonca, et al.

By

John P. Wagner, Jr.

Attorney/Agent for Applicant(s)

Reg No. : 35,398

Date : 11/09/2007

Telephone : 408-377-0500

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Mendonca et al.	Patent Application	
Serial No.:	10/627,017	Group Art Unit:	2136
Filed:	July 25, 2003	Examiner:	Okoronkwo, C.

For: METHOD OF MANAGING UTILIZATION OF NETWORK INTRUSION DETECTION SYSTEMS IN A DYNAMIC DATA CENTER

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellants.

Status of Claims

Claims 1-20 remain pending. Claims 1-20 have been rejected. This appeal involves Claims 1-20.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claims 1, 8 and 15 pertain to various embodiments of managing utilization of network intrusion detection systems in a dynamic data center. The instant application serial no. 10/627,017 states in the background section on page 2 lines 1-4 "...the capacity of the network intrusion detection systems may be underutilized or exceeded at various monitoring points, causing inefficient use of the network intrusion detection systems." The claims of the instant application recite embodiments for addressing this.

For example, independent Claims 1 and 8 recite,

> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
>
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
>
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

As described at page 5 lines 13-30 of the instant application, Figure 1 depicts a dynamic data center 100 with a plurality of network intrusion detection systems 70. Figure 1 also depicts networks 40 (e.g., net1, net2, net3, net4, and net5).

Referring to Figures 1 and 2, a description, according to one embodiment, of "providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center," as recited by independent Claims 1 and 8 is provided by the instant application on page 7 lines 8-18, which states,

> Figure 2 illustrates a flow chart showing a method 200 of managing utilization of network intrusion detection systems in a dynamic data center 100 in accordance with an embodiment of the present invention. Reference is made to Figure 1.
>
> At Step 210, the network intrusion detection systems in the network intrusion detection systems pool 70 are provided in a dynamic data center

> 100. Each network intrusion detection system in the network intrusion detection systems pool 70 is networked or pre-wired so that utilization of each network intrusion detection system can be based on demand for the network intrusion detection systems in the dynamic data center 100.

Referring to Figures 1 and 2, a description, according to one embodiment, of "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems ," as recited by independent Claims 1 and 8 is provided by the instant application on page 7 lines 20-24, which states,

> Further, at Step 220, a monitoring policy and a plurality of monitoring points to be monitored on a network with any of the network intrusion detection systems in the network intrusion detection systems pool 70 are received. In an embodiment, a graphical user interface is configured to receive the monitoring policy and the plurality of monitoring points to be monitored.

Referring to Figures 1, 2 and 3, a description, according to one embodiment, of "automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy," as recited by independent Claims 1 and 8 is provided by the instant application on page 7 line 27 to page 9 line 14, which states,

> At Step 230, the controller 10 automatically arranges the monitoring of the monitoring points using the network intrusion detection systems in the network intrusion detection systems pool 70 and the monitoring policy.
>
> Figure 3 illustrates a flow chart showing a method 300 of automatically arranging the monitoring of monitoring points in a network in accordance with an embodiment of the present invention. Moreover, Figure 3 provides additional details about the execution of Step 230 of Figure 2. Reference is made to Figure 1.
>
> At Step 310, the controller 10 automatically configures network resources from the network resources pool 60 and/or in the internal networks (e.g., net1, net2, net3, net4 and net5) to provide network communication data from the monitoring points to a plurality of available network intrusion detection systems from the network intrusion detection systems pool 70.
>
> Moreover, at Step 320, the controller 10 automatically configures the available network intrusion detection systems from the network intrusion detection systems pool 70 to receive the network communication data based on the monitoring policy.
>
> Furthermore, at Step 330, the controller 10 monitors the capacity of the network intrusion detection systems that are monitoring the monitoring points on the network.

Page 5 lines 14-28 describe that the controller 10 can automatically increase a number of particular network intrusion detection systems or automatically decrease a number of particular network intrusion detection systems.

Independent Claim 15 recites,

A system comprising:
a dynamic data center including:
a plurality of network resources;
a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (emphasis added).

As described at page 5 lines 13-30 of the instant application, Figure 1 depicts a dynamic data center 100 with a plurality of network intrusion detection systems 70 and network resources 60. Figure 1 also depicts networks 40 (e.g., net1, net2, net3, net4, and net5).

Referring to Figures 1 and 2, the instant application states at page 7 lines 8-18,

Figure 2 illustrates a flow chart showing a method 200 of managing utilization of network intrusion detection systems in a dynamic data center 100 in accordance with an embodiment of the present invention. Reference is made to Figure 1.

At Step 210, the network intrusion detection systems in the network intrusion detection systems pool 70 are provided in a dynamic data center 100. Each network intrusion detection system in the network intrusion detection systems pool 70 is networked or pre-wired so that utilization of each network intrusion detection system can be based on demand for the network intrusion detection systems in the dynamic data center 100.

A graphical user interface 20 is depicted on Figure 1. "a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems," (emphasis added) as recited by Claim 15 is described, among other places, at page 7 lines 20-24 as follows:

> Further, at Step 220, a monitoring policy and a plurality of monitoring points to be monitored on a network with any of the network intrusion detection systems in the network intrusion detection systems pool 70 are received. In an embodiment, a graphical user interface is configured to receive the monitoring policy and the plurality of monitoring points to be monitored.

A controller 10 is depicted on Figure 1. "a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy," (emphasis added) as recited by Claim 15 is described, among other places, at page 7 line 26 to page 8 line 14 as follows:

> At Step 230, the controller 10 automatically arranges the monitoring of the monitoring points using the network intrusion detection systems in the network intrusion detection systems pool 70 and the monitoring policy.
>
> Figure 3 illustrates a flow chart showing a method 300 of automatically arranging the monitoring of monitoring points in a network in accordance with an embodiment of the present invention. Moreover, Figure 3 provides additional details about the execution of Step 230 of Figure 2. Reference is made to Figure 1.
>
> At Step 310, the controller 10 automatically configures network resources from the network resources pool 60 and/or in the internal networks (e.g., net1, net2, net3, net4 and net5) to provide network communication data from the monitoring points to a plurality of available network intrusion detection systems from the network intrusion detection systems pool 70.
>
> Moreover, at Step 320, the controller 10 automatically configures the available network intrusion detection systems from the network intrusion detection systems pool 70 to receive the network communication data based on the monitoring policy.
>
> Furthermore, at Step 330, the controller 10 monitors the capacity of the network intrusion detection systems that are monitoring the monitoring points on the network.

Page 5 lines 14-28 describe that the controller 10 can automatically increase a number of particular network intrusion detection systems or

automatically decrease a number of particular network intrusion detection systems.

Grounds of Rejection to be Reviewed on Appeal

1. In paragraph 2 of the Office Action, Claims 1-20 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. patent no. 6,578,147 by Shanklin et al. (referred to herein as "Shanklin").

Arguments

1. Whether Claims 1-20 are anticipated by 35 U.S.C. 102(e) as being disclosed by Shanklin (6,578,147)

A. Scope and Content of the Cited Art Reference (Shanklin)

Referring to Shanklin's title and abstract, among other places, Appellants understand Shanklin to teach parallel intrusion detection sensors with load balancing for high speed networks where multiple sensors are connected at an internetworking device, which can be a router or a switch. Shanklin states in the abstract,

> ... Multiple sensors are connected at an internetworking device, which can be a router or a switch. The sensors operate in parallel and each receives a portion of traffic through the internet-working device, at a session-based level or at a lower (packet-based) level. Depending on the type of internet-working device (router or switch) the load balancing mechanism that distributes the packets can be internal or external to the internetworking device. Also depending on the level of packet distribution (session-based or packet based), the sensors share a network analyzer (if session-based) or both a network analyzer and a session analyzer (if packet-based).

B. Differences Between the Cited Art Reference and the Claimed Invention.

Independent Claim 1 recites,

> A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:
> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy. (emphasis added)

Appellants respectfully submit that Shanklin does not teach or suggest, among other things, "said network intrusion detection systems in said dynamic data center ...receiving a monitoring policy and a plurality of monitoring points to be

monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy," as recited by Claim 1

Referring to Shanklin's title and abstract, among other places, Appellants understand Shanklin to teach parallel intrusion detection sensors with load balancing for high speed networks where multiple sensors are connected at an internetworking device, which can be a router or a switch. The Office Action asserts that Shanklin teaches the embodiment recited by Claim 1 at Col. 1 line 63 through Col. 2 line 8. Col. 1 line 63 through Col. 2 line 8 states,

> One aspect of the invention is a method of detecting unauthorized access on a network as indicated by signature analysis of packet traffic on the network. A plurality of intrusion detection sensors are connected at a network entry point associated with an internetworking device, such as a router or switch. The packet load to the sensors is "load balanced", such that said packets are distributed at least at a session-based level. The load balancing may be at a lower (packet-based) level, which tends to more evenly distribute the load on each sensor but requires additional processing external to the sensors or requires sharing of session-level data between sensors. (emphasis added)

Shanklin does not mention a dynamic data center and therefore Appellants do not understand Shanklin to teach "said network intrusion detection systems in said dynamic data center," as recited by Claim 1. Further, Appellants do not understand Shanklin to mention a monitoring policy therefore Appellants do not understand Shanklin to teach "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems" nor to teach "automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy."

The Office Action does not state in the portion of the Office Action on page 4 pertaining to Claim 1 what in Shanklin teaches "a plurality of monitoring points" (emphsis added). For the sake of argument, Appellants shall assume that the Office Action intended to assert that Shanklin's "network entry points" (emphasis added) are analogous to Claim 1's "plurality of monitoring points" (this is not an admission on the part of Appellants). However, Appellants do not

understand Shanklin to teach receiving Shanklin's network entry points. Further, Appellants do not understand Shanklin to teach automatically arranging the monitoring of Shanklin's network entry points let alone teach automatically arranging the monitoring of Shanklin's network entry points using network intrusion detection systems and a monitoring policy. Lastly, Appellants do not understand Shanklin to teach that Shanklin's network entry points can be monitored with any network intrusion detection system.

RESPONSE TO ARGUMENTS

In paragraph 1.2, the Office Action states,

> In response to Applicant argument that the Shanklin et al. reference does not teach or suggest…arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy; the Examiner respectfully disagrees citing column 1 lines 37-48 and 64-66, which specifically recites, "signatures are stored, and in real time, compared to the packet flow incoming to the network" and "a plurality of intrusion detection sensors…connected at a network entry point associated with an internetworking device." This disclosure of 'signatures' is analogous to the claimed 'monitoring policy…(emphasis added).

The Office Action asserts in paragraph 1.2 that Shanklin's signatures teach Claim 1's monitoring policy. The Office Action appears to assert in paragraph 1.2 that Shanklin's network entry points teach Claim 1's monitoring points and that Shanklin's intrusion detection sensors teach Claim 1's network intrusion detection systems. However, Appellants do not understand Shanklin to teach receiving his signatures nor to teach receiving his network entry points. For example, at Col. 4 lines 5-8, Shanklin states, "A sensor 11 might also have the capability to be programmed to analyze packets for customized signatures for a particular network" (emphasis added). Since his sensors are programmed for customized signatures, Shanklin does not teach receiving his customized signatures. At Col. 4 lines 64-66, Shanklin states, "Context-oriented signatures consist of known network service vulnerabilities" (emphasis added). Since Shanklin programs his sensors for customized signatures it would also stand to reason that Shanklin would program his sensors for signatures that consist of known network service vulnerabilities. Further, Appellants do not understand Shanklin to automatically arrange the monitoring of his entry points using his signatures.

In paragraph 1.3, the Office Action states, "In response to Applicant argument that the Shanklin et al. reference does not teach or suggest a 'plurality of entry points'..." (emphasis added). The Office Action has misquoted Claim 1 and the previous response. Claim 1 recites "a plurality of monitoring points" (emphasis added). The Office Action goes on to state, "...the Examiner respectfully disagrees citing column 1 lines 64-66 which recite, specifically 'a plurality of intrusion detection sensors...'." In paragraph 1.2 the Office Action appeared to assert that Shanklin's entry points teach Claim 1's monitoring points. Now in paragraph 1.3 the Office Action is asserting that Shanklin's intrusion detection sensors teach Claim 1's monitoring points. Appellants do not understand Shanklin's entry points to teach Claim 1's monitoring points for reasons already provided herein. Appellants do not understand Shanklin's intrusion detection sensors to teach Claim 1's monitoring points, among other things, because Shanklin does not automatically arrange the monitoring of his intrusion detection sensors using his signatures.

The Office Action states in the last 2 sentences of paragraph 1.3, "The disclosed scalbility of the invention reads upon the claims of monitoring on 'any' network." The Office Action has misquoted Claim 1. Claim 1 recites, "...monitoring a network with any of said network intrusion systems..." (emphasis added).

CONCLUSION

In summary, Appellants respectfully submit that the Office Action's rejections of the claims are improper as the rejection of Claims 1-20 do not satisfy the requirements of a prima facie case of anticipation as claim features are not met by the cited reference. Accordingly, Appellants respectfully submit that the rejection of Claims 1-20 under 35 U.S.C. §102(e) are improper and should be reversed.

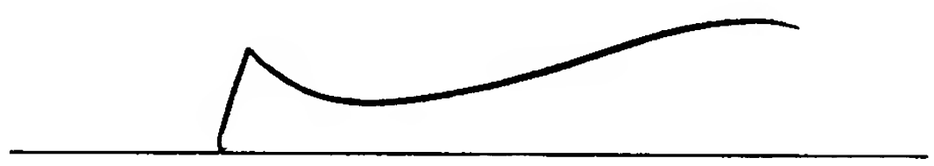
In summary, the Appellants respectfully request that the Board reverse the Examiner's rejections of Claims 1-20.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 11/9/2007



John P. Wagner

Registration Number: 35,398

WAGNER BLECHER LLP
Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076
408-377-0500

Claims Appendix

1. A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

2. The method as recited in Claim 1 wherein said automatically arranging the monitoring of said monitoring points includes:

automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and

automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

3. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

4. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

5. The method as recited in Claim 2 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

6. The method as recited in Claim 1 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

7. The method as recited in Claim 1 wherein said dynamic data center is a utility data center.

8. A computer-readable medium comprising computer-executable instructions stored therein for performing a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

9. The computer-readable medium as recited in Claim 8 wherein said automatically arranging the monitoring of said monitoring points includes:

automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and

automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

10. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

11. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

12. The computer-readable medium as recited in Claim 9 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

13. The computer-readable medium as recited in Claim 8 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

14. The computer-readable medium as recited in Claim 8 wherein said dynamic data center is a utility data center.

15. A system comprising:

a dynamic data center including:

a plurality of network resources;

a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

16. The system as recited in Claim 15 wherein said controller automatically configures said network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems, and wherein said controller automatically configures said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

17. The system as recited in Claim 16 wherein said controller automatically increases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

18. The system as recited in Claim 16 wherein said controller automatically decreases a number of particular network intrusion detection

systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

19. The system as recited in Claim 15 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

20. The system as recited in Claim 15 wherein said dynamic data center is a utility data center.

Evidence Appendix

None

Related Proceedings Appendix

None